Phishing Outline
==========

I. People/organizations involved in any phishing attack.

  A. Thieves: criminal gangs, individuals, mercenaries
  B. Unwitting participants: corporations, individuals
  C. Victims: end users, impersonated organization(s)
  D. White hats: IT staff, network admins, volunteers, law enforcement

II. Technologies employed to carry out the phishing attack.

  A. Botnets, trojans and remote controlled systems
  B. Email in the form of spam (HTML email in particular)
  C. DNS system (hijacking, compromised servers, lookalike names)
  D. Web servers (running the harvesting programs)

III. Phishing attack walkthrough (parenthesized numbers refer to diagram).

  A. Attacker compromises a DNS server, web server, bunch of desktops.
  B. Attacker creates lookalike web page with program to harvest data.
  C. Attacker sends phishing spam pointing to lookalike web page.
  E. End user receives spam (unfiltered?, filter subverted). (D1)
  F. End user visits look-alike web page; e.g. a banking site. (D2-5)
  G. End user enters login and password. (D6)
  H. Attacker stores login and password and redirects user back to
     valid site. (D7)

IV. Countermeasures.

  - Use antispyware, antispam and antivirus software.
  - Use Firefox, not Internet Explorer.
  - Suppress HTML portion of HTML mails.
  - Don't click on links in email.
  - Bookmark a site after you have
    - checked the location bar and SSL lock.
    - checked the certificate details.
  - Contact an online anti-phishing organization.
  - Contact your local FBI chapter.

V. Conclusions and questions

  Martin A. Brown <martin@linux-ip.net>